Amendments to the Claims

1. (original) A cryptographic key split combiner, comprising:

a) a plurality of key split generators for generating cryptographic key splits; and

b) a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key;

c) wherein each of said key split generators includes means for generating key splits from seed data.

2. (original) The cryptographic key split combiner of claim 1, wherein said plurality of key split generators includes a random split generator for generating a random key split based on reference data.

3. (original) The cryptographic key split combiner of claim 2, wherein said random split generator includes means for generating a random sequence based on the reference data.

4. (original) The cryptographic key split combiner of claim 2, wherein said random split generator includes means for generating a pseudorandom sequence based on the reference data.

5. (original) The cryptographic key split combiner of claim 2, wherein said random split generator includes means for generating a key split based on the reference data and on chronological data.

6. (original) The cryptographic key split combiner of claim 2, wherein said random split generator includes means for generating a key split based on the reference data and on static data.

7. (original) The cryptographic key split combiner of claim 6, further including means for updating the static data.

8. (original) The cryptographic key split combiner of claim 7, wherein the means for updating the static data includes means for modifying a prime number divisor of the static data.

9. (original) The cryptographic key split combiner of claim 1, wherein said plurality of key split generators includes a token split generator for generating a token key split based on label data.

10. (original) The cryptographic key split combiner of claim 9, further comprising means for reading the label data from a storage medium.

11. (original) The cryptographic key split combiner of claim 9, wherein the label data includes user authorization data.

12. (original) The cryptographic key split combiner of claim 9, wherein said token split generator includes means for generating a random sequence based on the label data.

13. (original) The cryptographic key split combiner of claim 9, wherein said token split generator includes means for generating a pseudorandom sequence based on the label data.

14. (original) The cryptographic key split combiner of claim 9, wherein said token split generator includes means for generating a key split based on the label data and on organization data.

15. (original) The cryptographic key split combiner of claim 9, wherein said token split generator includes means for generating a key split based on the label data and on static data.

16. (original) The cryptographic key split combiner of claim 15, further including means for updating the static data.

17. (original) The cryptographic key split combiner of claim 16, wherein the means for updating the static data includes means for modifying a prime number divisor of the static data.

18. (original) The cryptographic key split combiner of claim 1, wherein said plurality of key split generators includes a console split generator for generating a console key split based on maintenance data.

19. (original) The cryptographic key split combiner of claim 18, wherein said console split generator includes means for generating a random sequence based on the maintenance data.

20. (original) The cryptographic key split combiner of claim 18, wherein said console split generator includes means for generating a pseudorandom sequence based on the maintenance data.

21. (original) The cryptographic key split combiner of claim 18, wherein said console split generator includes means for generating a key split based on previous maintenance data and on current maintenance data.

22. (original) The cryptographic key split combiner of claim 18, wherein said console split generator includes means for generating a key split based on the maintenance data and on static data.

23. (original) The cryptographic key split combiner of claim 22, further including means for updating the static data.

24. (original) The cryptographic key split combiner of claim 22, wherein the means for updating the static data includes means for modifying a prime number divisor of the static data.

25. (original) The cryptographic key split combiner of claim 1, wherein said plurality of key split generators includes a biometric split generator for generating a biometric key split based on biometric data.

26. (original) The cryptographic key split combiner of claim 25, wherein said biometric split generator includes means for generating a random sequence based on the biometric data.

27. (original) The cryptographic key split combiner of claim 25, wherein said biometric split generator includes means for generating a pseudorandom sequence based on the biometric data.

28. (original) The cryptographic key split combiner of claim 25, wherein said biometric split generator includes means for generating a key split based on biometric data vectors and on biometric combiner data.

29. (original) The cryptographic key split combiner of claim 25, wherein said biometric split generator includes means for generating a key split based on the biometric data and on static data.

30. (original) The cryptographic key split combiner of claim 29, further including means for updating the static data.

31. (original) The cryptographic key split combiner of claim 30, wherein the means for updating the static data includes means for modifying a prime number divisor of the static data.

32. (original) The cryptographic key split combiner of claim 1, wherein the cryptographic key is a stream of symbols.

33. (original) The cryptographic key split combiner of claim 1, wherein the cryptographic key is at least one symbol block.

34. (original) The cryptographic key split combiner of claim 1, wherein the cryptographic key is a key matrix.

35. (original) A process for forming cryptographic keys, comprising:

a) generating a plurality of cryptographic key splits from seed data; and

b) randomizing the cryptographic key splits to produce a cryptographic key.

36. (original) The process of claim 35, wherein generating a plurality of cryptographic key splits includes generating a random key split based on reference data.

37. (original) The process of claim 36, wherein generating a random key split includes generating a random sequence based on the reference data.

38. (original) The process of claim 36, wherein generating a random key split includes generating a pseudorandom sequence based on the reference data.

39. (original) The process of claim 36, wherein generating a random key split includes generating a key split based on the reference data and on chronological data.

40. (original) The process of claim 36, wherein generating a random key split includes generating a key split based on the reference data and on static data.

41. (original) The process of claim 40, further including updating the static data.

42. (original) The process of claim 41, wherein updating the static data includes modifying a prime number divisor of the static data.

43. (original) The process of claim 35, wherein generating a plurality of cryptographic key splits includes generating a token key split based on label data.

44. (original) The process of claim 43, further comprising reading the label data from a storage medium.

45. (original) The process of claim 43, wherein the label data includes user authorization data.

46. (original) The process of claim 43, wherein generating a token key split includes generating a random sequence based on the label data.

47. (original) The process of claim 43, wherein generating a token key split includes generating a pseudorandom sequence based on the label data.

48. (original) The process of claim 43, wherein generating a token key split includes generating a key split based on the label data and on organization data.

49. (original) The process of claim 43, wherein generating a token key split includes generating a key split based on the label data and on static data.

50. (original) The process of claim 49, further including updating the static data.

51. (original) The process of claim 50, wherein updating the static data includes modifying a prime number divisor of the static data.

52. (original) The process of claim 35, wherein generating a plurality of cryptographic key splits includes generating a console key split based on maintenance data.

53. (original) The process of claim 52, wherein generating a console key split includes generating a random sequence based on the maintenance data.

54. (original) The process of claim 52, wherein generating a console key split includes generating a pseudorandom sequence based on the maintenance data.

55. (original) The process of claim 52, wherein generating a console key split includes generating a key split based on previous maintenance data and on current maintenance data.

56. (original) The process of claim 52, wherein generating a console key split includes generating a key split based on the maintenance data and on static data.

57. (original) The process of claim 56, further including updating the static data.

58. (original) The process of claim 56, wherein the updating the static data includes modifying a prime number divisor of the static data.

59. (original) The process of claim 35, wherein generating a plurality of cryptographic key splits includes generating a biometric key split based on biometric data.

60. (original) The process of claim 59, wherein generating a biometric key split includes generating a random sequence based on the biometric data.

61. (original) The process of claim 59, wherein generating a biometric key split includes generating a pseudorandom sequence based on the biometric data.

62. (original) The process of claim 59, wherein generating a biometric key split includes generating a key split based on biometric data vectors and on biometric combiner data.

63. (original) The process of claim 59, wherein generating a biometric key split includes generating a key split based on the biometric data and on static data.

64. (original) The process of claim 63, further including updating the static data.

65. (original) The process of claim 63, wherein updating the static data includes modifying a prime number divisor of the static data.

66. (currently amended) A storage medium, including the cryptographic key~~,~~ formed by the process of claim 35.

67. (currently amended) The ~~cryptographic key~~ storage medium of claim 66, ~~including~~ wherein the cryptographic key includes a stream of symbols.

68. (currently amended) The ~~cryptographic key~~ storage medium of claim 66, ~~including~~ wherein the cryptographic key includes at least one symbol block.

69. (currently amended) The ~~cryptographic key~~ storage medium of claim 66, ~~including~~ wherein the cryptographic key includes a key matrix.

70. (new) The storage medium of claim 66, comprising a magnetic storage medium.

71. (new) The storage medium of claim 70, comprising random access memory.